AMENDMENTS TO THE CLAIMS

1. (currently amended) A method of filtering data in a computer network, the method comprising:

receiving data in a first computer;

scanning the data against at least a portion of a knowledge base in the first computer;

forwarding the data to a second computer over a computer network; and

scanning the data against at least a portion of a knowledge base in the second computer, the portion of the knowledge base in the second computer including information not present in the portion of the knowledge base in the first computer;

wherein the knowledge base in the first computer is a subset of the knowledge base in the second computer;

wherein the knowledge base in the second computer has segments 1,2,3,...p, the knowledge base in the first computer has segments 1,2,3,...m, p is greater than or equal to m, the data are scanned from 1 to m in the first computer, and the data are scanned from m+1 to p, if p is greater than m, in the second computer.

2-8 (canceled)

9. The method of claim 1 wherein the data comprise a file.

10. (original) A system comprising:

a content filtering system in a first computer, the content filtering system being configured to determine a destination computer of an incoming data and to scan the incoming data against a knowledge base in the first computer based on a resource capacity of the destination computer; and

a content filtering agent in a second computer, the second computer being the destination computer of the of the incoming data, the content filtering agent being configured to scan the incoming data against a knowledge base in the second computer based on an amount of scanning performed by the content filtering system on the incoming data in the first computer.

11. (original) The system of claim 10 wherein the knowledge base in the first computer and the knowledge base in the second computer comprise a virus pattern file.

12. (original) The system of claim 10 wherein the knowledge base in the first computer and the knowledge base in the second computer comprise anti-spam related information.

13. (original) The system of claim 10 wherein the knowledge base in the first computer and the knowledge base in the second computer comprise unauthorized intrusion related information.

14. (original) The system of claim 10 further comprising:

a capacity mapping table in the first computer, the capacity mapping table being configured to indicate resource capacities of computers coupled to the first computer over a network.

15. (original) The system of claim 10 wherein the resource capacity comprises storage space.

16. (original) The system of claim 10 wherein the resource capacity comprises processor speed.

17. (original) The system of claim 10 wherein the first computer comprises an appliance performing antivirus functions.

18. (original) A method of detecting viruses in an incoming data, the method comprising:

comparing a content of an incoming data against a first set of virus patterns in a pattern file in a first computer serving as a gateway security node;

forwarding the incoming data to a second computer; and

comparing the content of the incoming data against a second set of virus patterns in a pattern file in a second computer, the second set of virus patterns including virus patterns that are different from that in the first set of virus patterns.

19. (original) The method of claim 18 wherein virus patterns in the first set of virus patterns are selected based on a resource capacity of the second computer.

20. (original) The method of claim 18 wherein the pattern file in the first computer is a subset of the pattern file in the second computer.

21. (new) A method of filtering data in a computer network, the method comprising:

receiving data in a first computer;

scanning the data against at least a portion of a knowledge base in the first computer;

forwarding the data to a second computer over a computer network; and

scanning the data against at least a portion of a knowledge base in the second computer, the portion of the knowledge base in the second computer including information not present in the portion of the knowledge base in the first computer;

wherein the knowledge base in the first computer and the knowledge base in the second computer comprise a virus pattern file.

22. (new) The method of claim 21 wherein the data comprise a file.

23. (new) A method of filtering data in a computer network, the method comprising:

receiving data in a first computer;

scanning the data against at least a portion of a knowledge base in the first computer;

forwarding the data to a second computer over a computer network; and

scanning the data against at least a portion of a knowledge base in the second computer, the portion of the knowledge base in the second computer including information not present in the portion of the knowledge base in the first computer;

wherein the data are scanned in the first computer and in the second computer for computer viruses.

24. (new) The method of claim 23 wherein the data comprise a file.

25. (new) A method of filtering data in a computer network, the method comprising:

receiving data in a first computer;

scanning the data against at least a portion of a knowledge base in the first computer;

forwarding the data to a second computer over a computer network; and

scanning the data against at least a portion of a knowledge base in the second computer, the portion of the knowledge base in the second computer including information not present in the portion of the knowledge base in the first computer;

wherein the data are scanned in the first computer and in the second computer for spam.

26. (new) The method of claim 25 wherein the data comprise a file.

27. (new) A method of filtering data in a computer network, the method comprising:

receiving data in a first computer;

scanning the data against at least a portion of a knowledge base in the first computer;

forwarding the data to a second computer over a computer network; and

scanning the data against at least a portion of a knowledge base in the second computer, the portion of the knowledge base in the second computer including information not present in the portion of the knowledge base in the first computer;

wherein the data are scanned in the first computer and in the second computer for unauthorized intrusion into the computer network.

28. (new) The method of claim 27 wherein the data comprise a file.